



A screen shot of a computer screen

AI-generated content may be incorrect.

A **firewall** is a security system that **monitors and controls incoming and outgoing network traffic** based on pre-defined security rules. It acts as a barrier between a trusted network (like your internal LAN) and untrusted networks (like the internet).

Here's how it filters traffic:

1. **Rules-Based Filtering**:  
   Firewalls use a list of rules to determine whether to allow or block network packets. Each rule is typically based on:
   * IP address (source or destination)
   * Port number (e.g., 80 for HTTP, 22 for SSH)
   * Protocol (TCP, UDP, etc.)
   * Direction (inbound or outbound)
2. **Default Policies**:
   * Most firewalls default to either **allow all** or **deny all** and then selectively override with rules.
   * For example, deny all + allow port 22 means only SSH is allowed.
3. **Traffic Direction**:
   * **Inbound rules** manage traffic coming *into* your machine.
   * **Outbound rules** manage traffic going *out* to the internet or other systems.
4. **Stateful Inspection**:
   * Many modern firewalls are **stateful**, meaning they track active connections and only allow return traffic that matches a known connection.
   * E.g., if you open a browser and access a site, the return data is allowed because the connection was initiated by you.

**Simple Example:**

If you configure a firewall to **deny port 23 (Telnet)**:

* Any external attempt to connect to your computer using Telnet will be blocked.
* If you then try telnet localhost 23, and the firewall is enabled, the connection fails.